

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

SUBJECT DEVICE-1 through SUBJECT DEVICE-9
(as identified in ATTACHMENT A)

Case No.

3:18-mj-724

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

See Attachment C

Offense Description

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig
Applicant's signature

Andrea R. Kinzig, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 11-2-18

City and state: Dayton, Ohio

Sharon L. Ovington
Judge's signature

Sharon L. Ovington, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The property to be searched is the following:

1. Custom desktop computer bearing serial number C615111502472, black in color ("SUBJECT DEVICE-1");
2. Samsung Galaxy Note8 cellular telephone bearing Model SM-N950U and IMEI 358503085026715, black in color ("SUBJECT DEVICE-2");
3. WD My Book external hard drive bearing serial number WCC4E7TZSXV3 ("SUBJECT DEVICE-3");
4. Adata Solid State Drive (SSD) bearing Model ASP610SS-256GM, 256 GB ("SUBJECT DEVICE-4");
5. SanDisk SD card, 256 MB ("SUBJECT DEVICE-5");
6. Micro Center flash drive, 16 GB ("SUBJECT DEVICE-6");
7. SanDisk Cruzer Blade flash drive, 8 GB ("SUBJECT DEVICE-7");
8. Red flash drive with no markings ("SUBJECT DEVICE-8"); and
9. SanDisk Cruzer flash drive, 4 GB ("SUBJECT DEVICE-9").

SUBJECT DEVICE-1 through SUBJECT DEVICE-9 are currently located at the Federal Bureau of Investigation, 7747 Clyn Road, Centerville, Ohio, 45459.

This warrant authorizes the forensic examination of SUBJECT DEVICE-1 through SUBJECT DEVICE-9 for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items evidencing violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography); and 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and distribution of child pornography.
2. Any visual depictions of minors.
3. Any Internet history indicative of searching for child pornography.
4. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any Internet or cellular telephone communications (including email, social media, etc.) with minors.
6. Evidence of utilization of the FreeChatNow website.
7. Evidence of utilization of the account name MRRSUGARB3AR.
8. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
9. Lists of computer and Internet accounts, including user names and passwords.
10. Any information related to Internet Protocol (IP) addresses, Wi-Fi accounts, and GPS data accessed by SUBJECT-DEVICE-1 through SUBJECT DEVICE-9.
11. Any information related to the use of aliases.
12. Evidence of user attribution showing who used or owned SUBJECT DEVICE-1 through SUBJECT DEVICE-9 at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.

ATTACHMENT C

Code Section

Offense Description

18 U.S.C. §2252(a)(4)(B) & (b)(1)

Possession of Child Pornography

18 U.S.C. §2252A(a)(5)(B) & (b)(1)

Possession of Child Pornography

18 U.S.C. §2252(a)(2)(B) & (b)(1)

Receipt and Distribution of Child Pornography

18 U.S.C. §2252A(a)(2) & (b)(1)

Receipt and Distribution of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I make this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — nine electronic devices — which are currently in law enforcement's possession, and the extraction from that property of electronically stored information described in Attachment B.
2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media including computer media.
3. Along with other agents, officers, and investigators of the Clark County (Ohio) Sheriff's Office and FBI, I am currently involved in an investigation of child pornography offenses committed by JEREMY MONTGOMERY (hereinafter referred to as "MONTGOMERY"). This Affidavit is submitted in support of an Application for a search warrant for the following:
 - a. Custom desktop computer bearing serial number C615111502472, black in color (hereinafter referred to as "**SUBJECT DEVICE-1**");
 - b. Samsung Galaxy Note8 cellular telephone bearing Model SM-N950U and IMEI 358503085026715, black in color (hereinafter referred to as "**SUBJECT DEVICE-2**");
 - c. WD My Book external hard drive bearing serial number WCC4E7TZSXV3 (hereinafter referred to as "**SUBJECT DEVICE-3**");
 - d. Adata Solid State Drive (SSD) bearing Model ASP610SS-256GM, 256 GB (hereinafter referred to as "**SUBJECT DEVICE-4**");
 - e. SanDisk SD card, 256 MB (hereinafter referred to as "**SUBJECT DEVICE-5**");

- f. Micro Center flash drive, 16 GB (hereinafter referred to as “**SUBJECT DEVICE-6**”);
 - g. SanDisk Cruzer Blade flash drive, 8 GB (hereinafter referred to as “**SUBJECT DEVICE-7**”);
 - h. Red flash drive with no markings (hereinafter referred to as “**SUBJECT DEVICE-8**”); and
 - i. SanDisk Cruzer flash drive, 4 GB (hereinafter referred to as “**SUBJECT DEVICE-9**”).
4. **SUBJECT DEVICE-1** through **SUBJECT DEVICE-9** are currently in the custody and control of the FBI, 7747 Clys Road, Centerville, Ohio, 45459. The purpose of the Application is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess child pornography; and 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive and distribute child pornography through interstate commerce. The items to be searched for and seized are described more particularly in Attachment B hereto.
5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the **SUBJECT DEVICE-1** through **SUBJECT DEVICE-9**.
7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B), and 2252A(a)(2) and (b)(1) are present within the information located on **SUBJECT DEVICE-1** through **SUBJECT DEVICE-9**.

PERTINENT FEDERAL CRIMINAL STATUTES

8. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or

transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

9. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
10. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
11. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

Background Information:

Definitions

12. The following definitions apply to this Affidavit and Attachment B to the Affidavit:
 - a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct,

- or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
- b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
 - d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
 - e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
 - f. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service

provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

- g. A network “**server**,” also referred to as a “**host**,” is a computer system that has been designated to run a specific server application or applications and provide requested services to a “client” computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.
- h. A “**client**” is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.
- i. “**Domain Name**” refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically “.com” for commercial organizations, “.gov” for the governmental organizations, “.org” for organizations, and “.edu” for educational organizations. Second level names will further identify the organization, for example “usdoj.gov” further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as “www.usdoj.gov,” to its currently assigned IP address (*i.e.*, 149.101.1.32), to enable the follow of traffic across the Internet.
- j. “**Log Files**” are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

- k. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- l. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- m. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- n. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Additional Technical Terms for Cellular Telephones:

- 13. The following additional technical terms related to cellular telephones apply to this Affidavit and Attachment B to the Affidavit:
 - a. A **“wireless telephone”** (or **“mobile telephone”**, or **“cellular telephone”**) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to

- enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. A “**digital camera**” is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
 - c. A “**GPS navigation device**” uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

Characteristics of Collectors of Child Pornography:

- 14. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
 - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

- b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
- c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
- d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Use of Computers and the Internet with Child Pornography

15. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in

which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.

- a. **Production:** Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.
- b. **Communication.** Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.
- c. **Distribution.** Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer

networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.

- d. **Storage.** The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

FreeChatNow Website

16. Based on Internet research, I have determined that FreeChatNow is a website located at www.freechatnow.com. The website's home page states that the website offers chat rooms based on sexuality and interest. Examples of chat rooms that are available on the website include Adult Chat, Singles Chat, Gay Chat, Roleplay Chat, Mobile Chat, Live Sex, Sex Chat, Lesbian Chat, Cam Chat, Cam Sex, Video Chat, and Chat Forums. The website's home page states that: "All of our chat rooms are intended for adults and the Sex Chat room contains explicit content".

BACKGROUND OF INVESTIGATION

17. On the evening of on or around October 20, 2018, the Clark County Sheriff's Office Communication Center received a telephone call from an adult female who will be referred to for purposes of this Affidavit as "Adult Female A". Adult Female A told the dispatcher that she had just seen pornographic pictures of children and young teenage girls on her live-in boyfriend's computer. Deputies of the Clark County Sheriff's Office were dispatched to Adult Female A's residence at 3955 Cabot Drive, Apartment B, in Springfield, Ohio to further investigate.
18. Upon arrival at Adult Female A's residence, deputies encountered Adult Female A, MONTGOMERY, and another adult female who will be referred to for purposes of this Affidavit as "Adult Female B". Deputies determined that Adult Female A and MONTGOMERY resided at the residence along with their two juvenile daughters, and that Adult Female B was visiting the residence.
19. Adult Female A agreed to be interviewed by a deputy, and she provided a written statement. Below is a summary of information provided by Adult Female A:

- a. Adult Female A had dated MONTGOMERY for approximately ten years, and they had two daughters. They currently resided together at 3955 Cabot Drive, Apartment B, in Springfield, Ohio.
 - b. Over the past few weeks, Adult Female A and MONTGOMERY had been having “issues”. Adult Female A suspected that MONTGOMERY was having a relationship with another woman. Earlier that evening, Adult Female A accessed MONTGOMERY’s computer (**SUBJECT DEVICE-1**) when he was away from the home to look for potential evidence of the suspected infidelity. Adult Female A found communications between MONTGOMERY and another woman, as well as file folders containing suspected child pornography.
 - c. After finding the suspected child pornography on MONTGOMERY’s computer, Adult Female A became “hysterical”. She contacted her cousin, Adult Female B, and asked that Adult Female B come to the residence. Adult Female A then contacted the Clark County Sheriff’s Office.
 - d. When MONTGOMERY returned to the home, Adult Female A questioned him about the suspected child pornography files. MONTGOMERY did not deny that he had child pornography on his computer.
20. Adult Female B also agreed to provide a written statement to deputies. Below is a summary of information provided by Adult Female B:
- a. Adult Female A contacted Adult Female B via telephone earlier that evening. Adult Female A sounded hysterical, and she asked Adult Female B to come to her residence.
 - b. When Adult Female B arrived at Adult Female A’s residence, Adult Female A showed Adult Female B images and videos on MONTGOMERY’s computer (**SUBJECT DEVICE-1**). Adult Female B advised that the images and videos depicted “very young children performing sexual acts”.
 - c. While Adult Female A and Adult Female B were looking at the files on MONTGOMERY’s computer, MONTGOMERY returned to the residence. MONTGOMERY appeared to be aware that Adult Female A had contacted the Clark County Sheriff’s Office. MONTGOMERY attempted to unplug the computer. MONTGOMERY then admitted that there was “stuff with children” on the computer. MONTGOMERY stated that he had these files on his computer because he “sold it to people”.

21. After being advised of his Miranda rights, MONTGOMERY agreed to be interviewed by Deputy Ronnie Lemen (one of the responding deputies) and to provide a written statement. Below is a summary of information provided by MONTGOMERY:
 - a. Before deputies arrived at his residence, MONTGOMERY was confronted by Adult Female A about pictures she found on his computer. The pictures depicted minor children who were nude or engaged in sexual acts. MONTGOMERY advised that these pictures were sent to him by someone else.
 - b. MONTGOMERY stated that child pornography files were presently located on his external hard drive (**SUBJECT DEVICE-3**).
 - c. MONTGOMERY denied that he ever produced or distributed child pornography files (although he later admitted to distributing child pornography, as detailed below).
22. Deputy Lemen requested that MONTGOMERY show him (Deputy Lemen) the child pornography files. MONTGOMERY agreed, and in the presence of Deputy Lemen, MONTGOMERY retrieved and external hard drive (**SUBJECT DEVICE-3**) from a closet in the loft area of his residence. MONTGOMERY attached the external hard drive (**SUBJECT DEVICE-3**) to a desktop computer (**SUBJECT DEVICE-1**) and showed Deputy Lemen multiple images of apparent child pornography.
23. Pursuant to MONTGOMERY's consent (which was memorialized on a Permission to Search form of the Clark County Sheriff's Office), deputies seized MONTGOMERY's desktop computer (**SUBJECT DEVICE-1**), his cellular telephone (**SUBJECT DEVICE-2**), and his external hard drive (**SUBJECT DEVICE-3**) from the residence.
24. MONTGOMERY agreed to travel to the Clark County Sheriff's Office to be further interviewed by Detective Deb Strileckyj. MONTGOMERY was again informed of his Miranda rights before he was interviewed. Below is a summary of information provided by MONTGOMERY:
 - a. MONTGOMERY again acknowledged that he had images of child pornography on his external hard drive (**SUBJECT DEVICE-3**). MONTGOMERY stated that the files depicted children who were approximately five to seventeen years old and who were engaged in sexual acts.
 - b. MONTGOMERY began viewing images of child pornography around February 2018. MONTGOMERY first received child pornography files from an individual with whom he was communicating on the FreeChatNow.com website.
 - c. The FreeChatNow.com website was the only website or application that MONTGOMERY utilized to receive and distribute child pornography files.

MONTGOMERY estimated that during the approximate time period of February 2018 through October 2018, he had downloaded and shared images of child pornography “on at least a dozen” occasions.

- d. MONTGOMERY estimated that he had least one hundred images of child pornography on his external hard drive (**SUBJECT DEVICE-3**). MONTGOMERY advised that he likely shared all of these files on the FreeChatNow.com website. MONTGOMERY shared child pornography files in order to receive more files in return.
 - e. MONTGOMERY’s user name on the FreeChatNow website was MRRSUGARB3AR. MONTGOMERY used the website to both communicate with adults about general sexually explicit topics and to trade child pornography files.
 - f. MONTGOMERY stated that he utilized both his desktop computer (**SUBJECT DEVICE-1**) and cellular telephone (**SUBJECT DEVICE-2**) to access the FreeChatNow website. MONTGOMERY stated that he only utilized the desktop computer to view, receive, and distribute child pornography files on this website. He used his cellular telephone to communicate on the website about general sexually explicit topics.
 - g. MONTGOMERY downloaded child pornography files he received from others on the FreeChatNow website to his external hard drive (**SUBJECT DEVICE-3**). He set up file folders to categorize the files that he saved. MONTGOMERY used a folder called “young” to save images depicting children who were approximately five to ten years old, a folder called “preteens” to save images depicting children who were approximately ten to thirteen years old, and a folder called “teens” to save images depicting children who were up to seventeen years old or possibly older.
 - h. MONTGOMERY denied that he ever produced child pornography or engaged in sexually explicit conduct with children.
 - i. MONTGOMERY was aware that viewing and trading child pornography was illegal.
25. On or around October 30, 2018, MONTGOMERY’s and Minor Female A’s two juvenile daughters were interviewed by an individual trained in conducting forensic interviews of children. The children will be referred to for purposes of this Affidavit as “Minor Female A” (who is four years old) and “Minor Female B” (who is six years old). The interviews were observed by Detective Strileckyj. Detective Strileckyj provided me with the following information regarding the interviews:

- a. Minor Female A's speech was difficult to understand. Although a number of Minor Female A's statements could not be understood, Detective Strileckyj and the interviewer were able to hear Minor Female A make statements about MONTGOMERY being naked, taking pictures of her, and showing her pictures of children who were not wearing clothing.
 - b. Minor Female B did not disclose any instances of sexual abuse by MONTGOMERY.
26. Adult Female A told Detective Strileckyj that MONTGOMERY primarily utilized his cellular telephone (**SUBJECT DEVICE-2**) to take photographs.
27. On or around October 31, 2018, Adult Female A contacted Detective Strileckyj. Adult Female A reported that she found an SDD hard drive (**SUBJECT DEVICE-4**), an SD card (**SUBJECT DEVICE-5**), and four flash drives (**SUBJECT DEVICE-6** through **SUBJECT DEVICE-9**) on the computer desk that MONTGOMERY utilized at their residence. Adult Female A voluntarily turned over **SUBJECT DEVICE-4** through **SUBJECT DEVICE-9** to Detective Strileckyj on or around November 1, 2018.
28. Based on all of the information detailed above, there is probable cause to believe that MONTGOMERY has possessed, received, and distributed child pornography. Based on statements made by Minor Female A, it is also reasonable to believe that MONTGOMERY may have produced or attempted to produce child pornography.
29. The electronic contents of **SUBJECT DEVICE-1** through **SUBJECT DEVICE-9** have not been accessed since the times that they were seized. The items were originally secured at the Clark County Sheriff's Office. I collected **SUBJECT DEVICE-1** through **SUBJECT DEVICE-3** from the Clark County Sheriff's Office on or around October 26, 2018. I collected **SUBJECT DEVICE-4** through **SUBJECT DEVICE-9** from the Clark County Sheriff's Office on or around November 2, 2018. The items are currently secured in the Evidence Control Room of the FBI's office located at 7747 Clio Road in Centerville, Ohio.
30. Based on my training and experience, I know that collectors of child pornography often maintain their collections for long periods of time. In addition, computer evidence typically persists for long periods of time, and computer data can often be recovered from deleted space (as further detailed below).
31. Based on my training and experience, I know that individuals are increasingly utilizing cellular telephones to do their computing. In my experience, I know that individuals involved in child pornography offenses often utilize both computer devices and their cellular telephones to obtain and store their child pornography files. Due to their portable nature, cellular telephones provide individuals easy access to their files.

32. In my experience, I know that due to the covert nature of the devices, individuals involved in child pornography offenses also utilize their cellular telephones to take photographs of children and produce child pornography. Based on my training and experience and examination of similar devices, I know that most cellular telephones have digital cameras.
- a. Examination of the exterior of the **SUBJECT DEVICE-2** indicates that it does in fact have a camera. As detailed above, Minor Female A reported that MONTGOMERY took photographs of her, apparently while he was naked. Also as detailed above, Adult Female A reported that MONTGOMERY primarily utilized his cellular telephone to take photographs.
33. Again based on my training and experience and examination of similar devices, I know that many cellular telephones and desktop computers (such as **SUBJECT DEVICE-1** and **SUBJECT DEVICE-2**) have the ability to connect to the Internet. I also know that many cellular telephones and desktop computers provide users with the ability to send and receive email messages. Individuals involved in child pornography offenses often utilize their cellular telephones and desktop computers to access Internet websites, exchange email messages, and access social media accounts to search for, view, and download child pornography.
34. Again based on my training and experience, I know that collectors of child pornography often use external devices (such as **SUBJECT DEVICE-3** through **SUBJECT DEVICE-9**) to store child pornography. The accumulation of child pornography files may fill up the space on the hard drives of computers, and external devices are needed to store and maintain files.
- a. As detailed above, MONTGOMERY identified that he utilized **SUBJECT DEVICE-3** to store his child pornography files.
- b. MONTGOMERY failed to disclose that he utilized **SUBJECT DEVICE-4** through **SUBJECT DEVICE-9** when he was interviewed, and he reported that he only utilized **SUBJECT DEVICE-3** to store child pornography files. Based on my training and experience, I know that child pornography offenders often attempt to conceal the devices they utilize to store child pornography files and/or that contain the most egregious content.
35. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

36. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chat rooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
37. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the computer devices located at the offenders' residences and on their cellular telephones.
38. In my experience, I know that many cellular telephones (such as **SUBJECT DEVICE-2**) store information related to IP addresses and Wi-Fi accounts that the telephone accessed and GPS data. This information helps in identifying the subjects' whereabouts during their criminal activities.
39. Based on all the information noted in this Affidavit, I submit there is probable cause to believe that **SUBJECT DEVICE-1** through **SUBJECT DEVICE-9** may contain evidence of MONTGOMERY's child pornography offenses.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

40. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.
41. There is probable cause to believe that things that were once stored on the **SUBJECT DEVICE-1** through **SUBJECT DEVICE-9** may still be stored there, for at least the following reasons:
 - a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

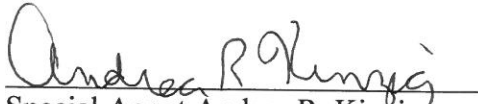
on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
 - c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
 - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
42. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT DEVICE-1** through **SUBJECT DEVICE-9** were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on **SUBJECT DEVICE-1** through **SUBJECT DEVICE-9** because:
- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

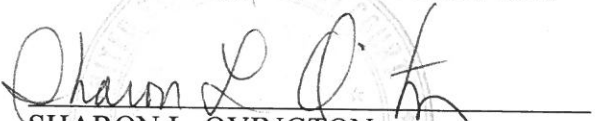
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
 - c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
 - d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
 - e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
43. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.
44. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement’s possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

45. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located on **SUBJECT DEVICE-1** through **SUBJECT DEVICE-9**, as described in Attachment A, in violation of 18 U.S.C. §§2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B), and 2252A(a)(2).
46. I, therefore, respectfully request that attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 2nd day of November 2018


SHARON L. OVINGTON
UNITED STATES MAGISTRATE JUDGE

